REMARKS

Reconsideration of the application in light of the above amendments and the following remarks is respectfully requested.

Status of the Claims

Claims 5-15 are pending. Claims 1-2 were previously canceled. Claims 3-4 have been withdrawn from consideration.

Claims 5 and 6 have been amended. Support for the amendments to claims 5 and 6 can be found in the Specification on page 1, paragraph 0003, page 4, paragraph 0014, and page 6, paragraph 0024-0026.

Claims 7-15 have been added. Claims 7-15 are directed to the elected Group II. Support for added claims 7-15 can be found in the Specification on page 5, paragraph 0017 through page 7, paragraph 0026.

No new matter has been added.

Objection to the Specification

The Examiner has objected to the Specification for containing minor informalities. Applicants have amended the Specification to fix minor typographical inaccuracies. Reconsideration and withdrawal of the objection is respectfully requested.

Rejection Under 35 U.S.C. §101

Claims 5 and 6 stand rejected under 35 U.S.C. §101 because the Examiner contends that the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner contends that claims 5 and 6 are directed to methods for establishing a key, the result of which is the determination of a common key, which produces neither a physical transformation, nor a concrete, tangible, and useful result. The Examiner contends that the methods recited in claims 5 and 6 are directed only to an abstract idea. Applicants respectfully traverse the rejection.

Applicants submit that it is well-known in the art of cryptography that the establishment of a common key has the practical application of allowing the respective subscribers to communicate securely over communication channels while ensuring that only the intended recipient can read the communication. See, Specification, page 1, paragraphs 0002-0003. It is respectfully submitted that an encryption key is useful for transmitting messages over a communication channel. Establishment of a common key for communication as described above is thus a "practical application in the technological arts." See MPEP §2106 IV.B.2(b)(ii). Therefore, Applicants submit that the methods recited in claims 5 and 6 produce a concrete, tangible, and useful result, as would be apparent to those of ordinary skill in the art.

Notwithstanding the above remarks, Applicants have amended independent claim 5 to recite that the claimed method is "for transmitting messages over a communication channel" and that the encryption key is "useable for transmitting messages over a communication channel." Applicants submit that using the common key for transmitting messages is a concrete, tangible, and useful result, and therefore the claimed subject matter is statutory.

Reconsideration and withdrawal of the rejection 35 U.S.C. §101 is respectfully requested.

Rejection Under 35 U.S.C. § 112, second paragraph

Claims 5 and 6 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

The Examiner contends that the variable "n" has not been defined in the claims. Applicants have amended independent claim 5 to recite that "n" represents the number of subscribers in the group of at least three subscribers.

With respect to the Examiner's contention specified in the Detailed Action, Item 7, page 4, line 10 through page 5, line 4, the Examiner contends that it is unclear "how each subscriber Ti (i ≠ 1) has access to the values Nj, where j ≠ 1. . . Furthermore, it is not clear how the subscriber Ti (i ≠ 1) have access to the random number z1." (Detailed Action, Item 7, page 4, lines 10-13.) The Examiner contends that "it appears that steps are missing which would provide for the receipt by each subscriber Ti of the values Nj (j ≠ 1) and also for the receipt or calculation of the symmetric decryption key that would allow decryption of the encrypted random number z1." (Detailed Action, Item, 7, page 4, line 21 though page 5, line 2.) Applicants respectfully traverse the rejection.

Applicants respectfully note that in the method recited in claim 5, it is not necessary for each subscriber Tj (j ≠ 1) to have direct access to the random number z1. As recited in the claim, each subscriber generates a respective message Nj, which is based on a respective random number zj. Then, each subscriber Tj, j ≠ 1, transmits its respective message Nj to the first subscriber $T_{1,}$ as recited in the "sending the respective message" step of claim 5. After receiving the messages Nj from each of the other subscribers Tj, j ≠ 1, the first subscriber T_1 creates a respective transmission key k^{1j} for each of the subscribers T_j, j ≠ 1, as recited in the encrypting step of claim 5. The first subscriber T1 then sends the encrypted random number z1 to all the other subscribers Tj, j ≠ 1, by generating a message M_{1j}. As recited in claim 5, the message M_{1j} is created using "a symmetrical encryption algorithm in which the random number z1 is encrypted with the transmission key k^{1j}."

Thus, when each subscriber Tj, $j \neq 1$, receives the message M_{1j} which contains the encrypted random number z1, the respective subscriber Tj, $j \neq 1$, is able to decrypt the encrypted random number z1 because $k^{1j} = k^{j1}$, *i.e.*, $(g^{z1})^{zj} = (g^{zj})^{z1}$. See, Specification, page 5, paragraph 0018. Each subscriber Tj is then able to calculate a common key $k{:=}h(z1, g^{z2} \ldots g^{zn})$ because $h(x1, x2 \ldots xn)$ has the property that it is symmetrical in its arguments. See, Specification, paragraph 0026. Therefore, by having the encrypted random number z1 in message M_{1j}, each subscriber Tj is able to decrypt the value of z1 using the properties of the symmetrical encryption algorithm, as explained above.

The Specification gives the example where there are three subscribers in the group, and $h(z1, g^{z2} \ldots g^{zn}) = g^{z1 \cdot z1} \cdot g^{z2 \cdot z1} \ldots\ g^{zn \cdot z1}$. See, Specification, paragraph 0026. In this example, after the generating step recited in claim 5, the first subscriber T_1 will have received $N_2 = g^{z2}$ mod p and $N_3 = g^{z3}$ mod p. The first subscriber T_1 then encrypts N_2 and N_3 to create k^{12} and k^{13}, and transmits the random number z1 encrypted in the form of M_{12} and M_{13} using transmission keys k^{12} and k^{13} to subscribers T_2 and T_3. T_2 and T_3 each decrypt the random number z1 using the property that $k^{ij} = (g^{zi})^{zj} = (g^{zj})^{zi}$ (*i.e.*, T_2 knows that $(g^{z2})^{z1} = (g^{z1})^{z2}$, and thus, T_2 can determine the random number z1; likewise with T_3.)

At this point, T_2 knows z1, z2, and has $(g^{z3})^{z1}$ from M_{13}. Likewise, T_3 knows z1, z3 and has $(g^{z2})^{z1}$ from M_{12}. T_1 also knows z1, and has $(g^{z2})^{z1}$ and $(g^{z3})^{z1}$ because T_1 received $N_2 = g^{z2}$ mod p and $N_3 = g^{z3}$ mod p. Thus, each of the subscribers T_1, T_2, and T_3 have all of the necessary information to calculate the common key k, because each subscriber T_1, T_2, and T_3 has sufficient information to substitute the values of $g^{z1 \cdot z1}$, $g^{z2 \cdot z1}$ and $g^{z3 \cdot z1}$ to determine the common key k. Each of the subscribers T_1, T_2, T_3 can determine the value of $g^{z1 \cdot z1}$, and T_2 and T_3 can calculate $g^{z2 \cdot z1}$ and

$g^{z2 \cdot z1}$, respectively. Although T_2 does not actually know the value of z3, T_2 has the value of $(g^{z3})^{z1}$, and therefore can calculate k. Likewise, although T_3 does not actually know the value of z2, T_3 has the value of $(g^{z2})^{z1}$, and therefore can calculate k.

Thus, it is clear that each of the subscribers T_j, $j \neq 1$ does not need to have direct access to the random number z1, and by having only the encrypted version of z1, each of the subscribers Tj is able to calculate the common key k. Applicants submit that claim 5 recites the necessary steps for carrying out the claimed invention, and therefore, is not indefinite.

With respect to the Examiner's rejection regarding the variable "k^{j1n}" recited in claim 6, Applicants respectfully note that claim 6 does not appear to recite such a variable. Applicants submit that claim 6 recites the variable "$k^{1j} = k^{j1}$" which has been defined in base claim 5. With respect to the Examiner's rejection regarding the feature of "the key" recited in claim 6, Applicants have amended claim 6 to have proper antecedent basis.

In view of the above remarks, Applicant respectfully requests reconsideration and withdrawal of the rejection under 35 U.S.C. §112, second paragraph.

New Claims

New claims 7-15 are directed to subject matter similar to that recited in claims 5 and 6. Support for added claims 7-15 can be found in the Specification on page 5, paragraph 0017 through page 7, paragraph 0026. It is respectfully submitted that new claims 7-15 are patentable.

CONCLUSION

Each and every point raised in the Office Action mailed August 10, 2006 has been addressed on the basis of the above remarks. In view of the foregoing it is believed that claims 5-15 are in condition for allowance and it is respectfully requested that the application be reconsidered and that all pending claims be allowed and the case passed to issue.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

Dated: November 10, 2006

Respectfully submitted,

By E. R. Swanson

Erik R. Swanson
Registration No.: 40,833
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant